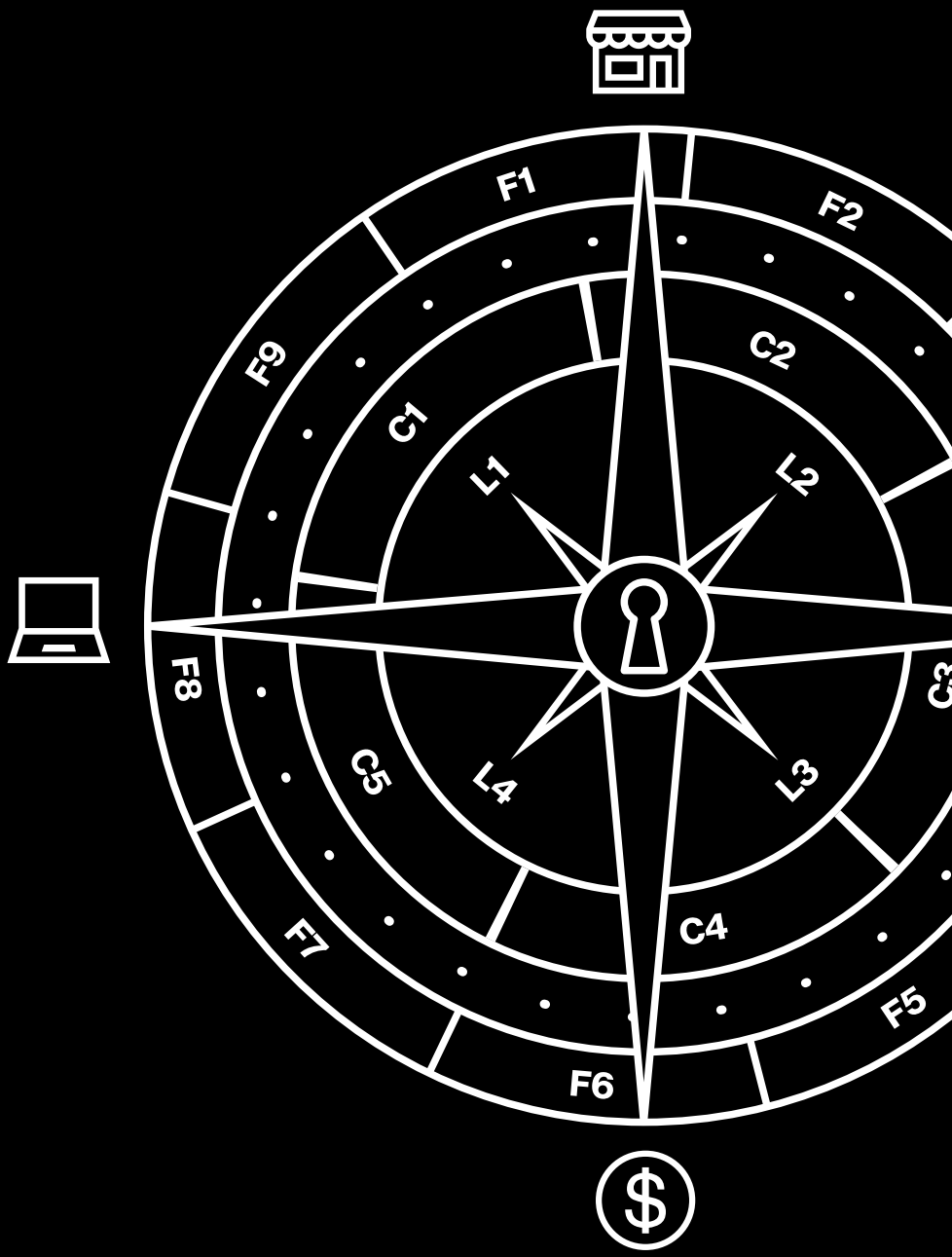
Payment Security Report 2019

Überblick über das Hotel- und Gaststättengewerbe



verizon

Im Hotel- und Gaststättengewerbe dreht sich alles um den Kunden. Doch statt Kunden wie Könige zu behandeln, setzen die Unternehmen sie mehr Cyberbedrohungen aus als alle anderen Branchen, die wir für den Verizon Payment Security Report (PSR) 2019 untersucht haben.

Im PSR 2019 finden Sie detailliertere Informationen zu Datenschutzverletzungen, die aus Untersuchungen des VTRAC-Ermittlungsteams (Verizon Threat Research Advisory Center) stammen. Die PCI-DSS-Compliance (Payment Card Industry Data Security Standard) sank im Hotel- und Gaststättengewerbe von 42,9 % im Bericht 2017 auf 38,5 % im letzten Jahr und 26,3 % im PSR 2019. Die Langzeittrends zeigen, dass Unterkünfte, Reiseveranstalter und Buchungsservices besonders häufig zum Opfer von Angriffen werden. Angesichts der Schlagzeilen über Datenlecks in mehreren bekannten Hotels sollten die Compliance-Richtlinien für den Schutz von Zahlungskartendaten in dieser Branche so bald wie möglich überprüft und überarbeitet werden.

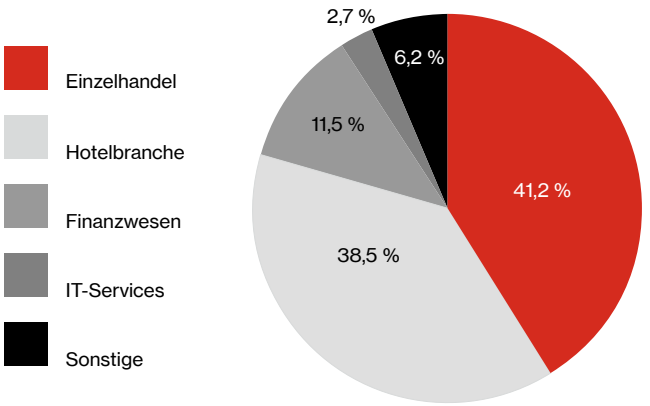


Abbildung 1: Bestätigte Datenschutzverletzungen nach Branche, Sechsjahrestrend, weltweite Verizon PFI-Einsätze (PCI Forensic Investigations) 2010–2016

Der Schutz von Zahlungskartendaten ist unverzichtbar – aber trotzdem erreichen nicht alle Unternehmen eine vollständige Compliance.

Verizon veröffentlicht den PSR seit neun Jahren. Bis 2017 stieg die Rate für die vollständige PCI-DSS-Compliance Jahr für Jahr in allen Branchen, doch seitdem geht sie zurück. Andere QSA-Unternehmen (Qualified Security Assessor) verzeichnen einen ähnlichen Rückgang bei der vollständigen Compliance. Im Hotel- und Gaststättengewerbe ist dieser Trend stärker als in allen anderen untersuchten Branchen.

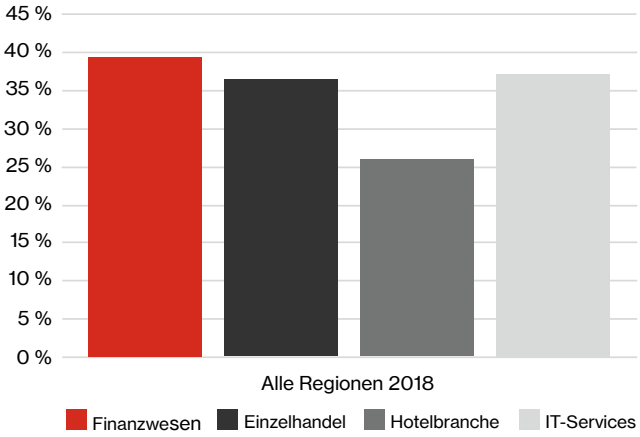


Abbildung 2: Weltweite Compliance nach Branche

Was ist PCI DSS?

Führende Kartenanbieter haben den Payment Card Industry Data Security Standard (PCI DSS) zur Vermeidung des Betrugs bei Kartenzahlungen eingeführt. Dabei geht es vorrangig um den Schutz der Kartendaten, aber der Standard basiert auf grundlegenden Sicherheitsprinzipien, die für alle Datentypen gelten. Es werden beispielsweise Aufbewahrungsrichtlinien, Verschlüsselungsmethoden, physische Sicherheitsmaßnahmen, Authentifizierungsmethoden und Zugangskontrollen abgedeckt. Weitere Informationen finden Sie unter pcisecuritystandards.org.

Trotz dieses Abwärtstrends blieb die Kontrolllücke (die angibt, wie weit Unternehmen von der vollständigen PCI-DSS-Compliance entfernt sind) mit 7,2 % gegenüber dem Vorjahr unverändert. Betrachtet man nur die Unternehmen, die die Interimsprüfung nicht bestanden haben, zeigt sich eine positivere Entwicklung. Im PSR 2019 ist die Kontrolllücke im Vergleich zum Vorjahr um 6,2 Prozentpunkte auf 10,2 % geschrumpft.

Unternehmen im asiatisch-pazifischen Raum (APAC-Region) schneiden besser ab: 69,6 % erzielten eine vollständige Compliance. In Europa, dem Nahen Osten und Afrika (EMEA-Region) erreichten 48,4 % vollständige Compliance. In Nord- und Südamerika sind es hingegen nicht einmal ein Viertel aller Unternehmen (20,4 %).

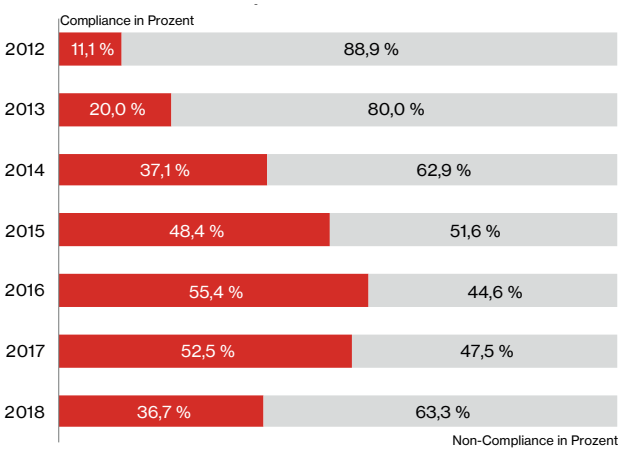


Abbildung 3: Vollständige Compliance nach Jahr

Der branchenübergreifende Rückgang der vollständigen Compliance macht deutlich, wie wichtig ausgereifte PCI-DSS-Compliance-Programme sind. Um vollständige Compliance zu erreichen, müssen Datenschutz- und Compliance-Programme (Data Protection and Compliance Programs, DPCPs) entwickelt und kontinuierlich aktualisiert werden. Für den PSR 2018 haben wir ca. 55 Unternehmen befragt und branchenübergreifend gaben 18 % an, kein DPCP zu besitzen. Keines der Unternehmen mit einem DPCP bewertete den Reifegrad des Programms als „optimiert“.

18 % der Unternehmen aller Branchen haben kein offizielles Datenschutz- und Compliance-Programm (DPCP). Keines der Unternehmen mit einem DPCP bewertete den Reifegrad des Programms als „optimiert“.

Proaktive Trendumkehr

Der Schutz von Kunden- und Karteninhaberdaten ist ein deutlicher Wettbewerbsvorteil. Den erreichen Unternehmen jedoch nur, wenn sie proaktiv statt reaktiv handeln. Verizon veröffentlicht den PSR 2019, um Unternehmen dabei zu unterstützen.

Der Bericht liefert einzigartige Einblicke in die Welt der Zahlungskartentransaktionen. Außerdem erklären wir darin, wie sich mit neuen richtungsweisenden Tools und Leitfäden, beispielsweise dem Verizon 9-5-4 Compliance Program Performance Evaluation Framework, der Schutz der PCI-Daten und die PCI-DSS-Compliance verbessern lassen.

Die Ergebnisse für das Hotel- und Gaststättengewerbe

Positive Ergebnisse

Das Gaststätten- und Hotelgewerbe hat sich in einigen Bereichen durchaus verbessert.

Bezüglich der Verschlüsselung der Daten bei der Übertragung (PCI-DSS-Anforderung 4) liegt es zwar nach wie vor auf dem letzten Platz, war aber die einzige Branche, die in diesem Bereich eine Verbesserung im Vergleich zum Vorjahr aufweisen konnte. Bei dem Schutz vor Malware (Anforderung 5) hat sich die Branche von allen Sektoren am meisten verbessert und eine Compliance-Rate von 84,2 % erzielt.

Sie war außerdem die einzige der für den PSR 2019 untersuchten Branchen, in der eine Verbesserung bei der Kontrolle des physischen Zugriffs (Anforderung 9) zu verzeichnen war. Sie stieg um 9,3 Prozentpunkte im Vergleich zum Vorjahr, auf 63,2 %.

Negative Ergebnisse

Das Hotel- und Gaststättengewerbe schnitt von den vier untersuchten Branchen (Hotel- und Gaststättengewerbe, Finanzdienstleister, Einzelhandel und IT-Services) bei mehreren wichtigen PCI-DSS-Anforderungen am schlechtesten ab:

- Wartung einer Firewall-Konfiguration (Anforderung 1)
- Änderung der Standardeinstellungen des Herstellers (Anforderung 2)
- Schutz gespeicherter Karteninhaberdaten (Anforderung 3)
- Verschlüsselung der Daten bei der Übertragung (Anforderung 4)
- Entwicklung und Wartung sicherer Systeme (Anforderung 6)
- Beschränkung des Zugriffs (Anforderung 7)
- Tests der Sicherheitssysteme und -prozesse (Anforderung 11)

Das Hotel- und Gaststättengewerbe erreichte nicht nur eine geringe Compliance in Bezug auf diese Anforderungen, die Branche wies auch die größte Kontrolllücke für die Anforderungen 1, 2, 6 und 11 sowie die stärkste Vergrößerung der Kontrolllücke für die Anforderungen 3, 6, 7 und 11 auf.

Unter all diesen nicht so guten Nachrichten möchten wir drei Bereiche hervorheben, in denen die Testergebnisse sich besonders stark verschlechtert haben: die Entwicklung und Wartung sicherer Systeme (um 21,9 Prozentpunkte), die Beschränkung des Zugriffs (um 21,5 Prozentpunkte) und die Authentifizierung des Zugriffs (Anforderung 8, Rückgang der vollständigen Compliance um 11,7 Prozentpunkte auf 42,1 %).

Da die Branche diese Anforderungen zuvor erfüllt hatte, deutet dies nicht auf ein allgemeines Problem mit einer Compliance-Vorgabe hin, sondern auf Schwierigkeiten bei der Entwicklung und Pflege eines ausgereiften PCI-DSS-Programms mit konsistenten Kontrollmaßnahmen.

Interessante Ergebnisse

Die Branche ist ein Rückzügler in Bezug auf den Schutz gespeicherter Karteninhaberdaten (Anforderung 3), hat allerdings auch mit besonders schwierigen Bedingungen zu kämpfen. Es gibt beispielsweise keine ausgereiften Lösungen für ihre speziellen Umgebungen.

Die angemessene Reaktion auf Angriffe ist ebenso wichtig wie deren Vermeidung. Laut den Ergebnissen des PSR hatte die Branche die größten Probleme mit der Benutzeridentifizierung und -authentifizierung (Prüfverfahren 10.2.5), der Prüfung und den Tests des Vorfallreaktionsplans (Prüfverfahren 12.10.2) und der Schulung der Mitarbeiter, die für die Reaktion auf Sicherheitsverletzungen verantwortlich sind (Prüfverfahren 12.10.4).

Warum ist die Erfüllung der PCI-DSS-Anforderungen so wichtig?

Wir haben PCI-DSS-Compliance und Sicherheitsverletzungen in Bezug auf Zahlungskartendaten ab dem Jahr 2008 abgeglichen und keinen einzigen Fall gefunden, in dem ein Unternehmen, das zum Zeitpunkt des Vorfalls alle 12 PCI-DSS-Anforderungen erfüllte, einen Verlust von Zahlungskartendaten erlitt.

Empfehlungen

Beschränken Sie den Zugriff

Den größten Rückgang in der Compliance-Rate verzeichnete die Branche in Bezug auf die Beschränkung des Zugriffs und die Authentifizierung. Doch diese Probleme lassen sich einfach beheben, denn es gibt zahlreiche Anbieter und Lösungen für derartige Funktionen. Das Verizon 9-5-4 Compliance Program Performance Evaluation Framework kann dabei ebenfalls helfen.

Investieren Sie in ausgereifte Sicherheitslösungen

Für mehrere PCI-DSS-Anforderungen sank die Compliance im Hotel- und Gaststättengewerbe. Für uns deutet das darauf hin, dass der aktuelle reaktive Ansatz durch ausgereiftere, konsistente Prozesse ersetzt werden sollte, die mit den Innovationen im Bereich der Zahlungssicherheit Schritt halten können.

Wie lässt sich das erreichen?

Die nächste Empfehlung enthält die ersten Schritte.

Abbildung 4: Relationales Modell der neun Faktoren der Kontrolleffektivität und -nachhaltigkeit

Entwicklung der Programmreife

Unternehmen verzichten nicht absichtlich auf gute Compliance-Programme. Die Entwicklung eines guten, ausgereiften Programms ist schwierig, aber mit den richtigen Leitfäden durchaus möglich.

Im PSR 2019 stellen wir das Verizon 9-5-4 Compliance Program Performance Evaluation Framework vor. Darin werden die Erkenntnisse aus früheren PSR und zusätzliche Tipps zu einem integrierten Framework zusammengefasst, das Unternehmen bei der Verbesserung des Datenschutzes und ihrer Compliance-Programme unterstützen soll. Das Framework ermöglicht eine größere Transparenz und Kontrolle, damit Unternehmen Wiederholbarkeit, Konsistenz und vorhersehbare Ergebnisse erzielen und Compliance gewährleisten können.

Integrieren Sie die Zahlungssicherheit

Im Gaststätten- und Hotelgewerbe dreht sich alles um das Wohlbefinden der Gäste und dazu gehören auch der Schutz und der sichere Umgang mit ihren Zahlungskartendaten. Sicherheitsbewussten Unternehmen eröffnen sich ganz neue Möglichkeiten. Wenn Unternehmen ein konsistentes Datenschutz- und Kontrollprogramm entwickeln, können sich ihre Kunden tatsächlich entspannen, da sie ihre Daten in Sicherheit wissen.

Weitere Informationen:

Wenn Sie wissen möchten, wie Sie Ihre Sicherheitsmaßnahmen und Ihr Compliance-Programm verbessern können, besuchen Sie unsere Website unter enterprise.verizon.com/resources/reports/payment-security/ oder wenden Sie sich an Ihren Verizon-Ansprechpartner.

verizon